channels should be used to address alleged departures from established reciprocity requirements and should resolve all, including the most egregious instances of non-compliance.

(d) Two complementary mechanisms are hereby established to augment existing organizational channels: (1) An accessible and responsive venue for reporting and resolving complaints/reported instances of non-compliance. Government and industry reporting channels shall be as follows:

(1) *Governnment.* (A) Agency employees are encouraged to bring suspected departures from applicable reciprocity requirements to the attention of the appropriate security authority in accordance with established agency procedures.

(B) Should the matter remain unresolved, the complainant (employee, Security Officer, Special Security Officer, or similar official) is encouraged to report the matter formally to the Senior Agency Official for resolution.

(C) Should the Senior Agency Official response be determined inadequate by the complainant, the matter should be reported formally to the Director, Security Policy Board Staff (D/SPBS). The D/SPBS, may revisit the matter with the Senior Agency Official or refer the matter to the Security Policy Forum as deemed appropriate.

(D) Should the matter remain unresolved, the Security Policy Forum may consider referral to the SPB, the agency head, or the National Security Council as deemed appropriate.

(ii) *Industry.* (A) Contractor employees are encouraged to bring suspected departures from the reciprocity provisions of the NISPOM to the attention to their Facility Security Officer (FSO) or Contractor Special Security Officer (CSSO), as appropriate, for resolution.

(B) Should the matter remain unresolved, the complainant (employee, FSO, or CSSO) is encouraged to report the matter formally to the Cognizant Security Office (CSO) for resolution.

(C) Should the CSO responses be determined inadequate by the complainant, the matter should be reported formally to the Senior Agency Official within the Cognizant Security Agency (CSA) for resolution.

(D) Should the Senior Agency Official response be determined inadequately by the complainant, the matter should be reported formally to the Director, information Security Oversight Office (ISOO) for resolution.

(E) The Director, ISOO, may revisit the matter with the Senior Agency Official or refer the matter to the agency head or the National Security Council as deemed appropriate.

(2) An annual survey administered to a representative sampling of agency and private sector facilities to assess overall effectiveness of agency adherence to applicable reciprocity requirements.

(i) In coordination with the D/SPBS, the Director, ISOO, as Chairman of the NISP Policy Advisory Committee (NISPPAC), shall develop and administer an annual survey to a representative number of cleared contractor activities/employees to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(ii) In coordination with the NISPPAC, the D/SPBS shall develop and administer an annual survey to a representative number of agency activities/personnel to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(iii) The goal of annual surveys should not be punitive but educational. All agencies and departments have participated in the crafting of these facilities policies, therefore, non-compliance is a matter of internal education and direction.

(e) Agencies will continue to review and assess the potential value added to the process of co-use of facilities by development of electronic data retrieval across government.

PART 149—POLICY ON TECHNICAL SURVEILLANCE COUNTERMEASURES

Sec.

AUTHORITY: E.O. 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391.)

SOURCE: 63 FR 4583, Jan. 30, 1998, unless otherwise noted.

§ 149.1 Policy.

(a) Heads of federal departments and agencies which process, discuss, and/or store classified national security information, restricted data, and sensitive but unclassified information, shall, in response to specific threat data and based on risk management principles, determine the need for Technical Surveillance Countermeasures (TSCM).

To obtain maximum effectiveness by the most economical means in the various TSCM programs, departments and agencies shall exchange technical information freely; coordinate programs; practice reciprocity; and participate in consolidated programs, when appropriate.

§ 149.2 Responsibilities.

(a) Heads of U.S. Government departments and agencies which plan, implement, and manage TSCM programs shall:

(1) Provide TSCM support consisting of procedures and countermeasures determined to be appropriate for the facility, consistent with risk management principles.

(2) Report to the Security Policy Board, attention: Chair, Facilities Protection Committee (FPC), for appropriate dissemination, all-source intelligence that concerns technical surveillance threats, devices, techniques, and unreported hazards, regardless of the source or target, domestic or foreign.

(3) Train a professional cadre of personnel in TSCM techniques.

(4) Ensure that the FPC and Training and Professional Development Committee are kept apprised of their TSCM program activities as well as training and research and development requirements.

(5) Assist other departments and agencies, in accordance with federal law, with TSCM services of common concern.

(6) Coordinate, through the FPC, proposed foreign disclosure of TSCM equipment and techniques.

(b) The FPC shall advise and assist the Security Policy Board in the development and review of TSCM policy, including guidelines, procedures, and instructions. The FPC shall:

(1) Coordinate TSCM professional training, research, development, test, and evaluation programs.

(2) Promote and foster joint procurement of TSCM equipment.

(3) Evaluate the impact on the national security of foreign disclosure of TSCM equipment or techniques and recommend policy changes as needed.

(4) Develop guidance for use in obtaining intelligence information on the plans, capabilities and actions of organizations hostile to the U.S. Government concerning technical penetrations and countermeasures against them.

(5) Biennially, review, update and disseminate the national strategy for TSCM.

§ 149.3 Definitions.

Classified National Security Information (CNSI). Information that has been determined pursuant to Executive Order 12958 (60 FR 19825, 3 CFR 1995 Comp., p. 333) or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Restricted Data (RD). All data concerning design, manufacture or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 102 of the Atomic Energy Act of 1954, as amended.

Sensitive but Unclassified. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Technical Surveillance Countermeasures (TSCM). Techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to classified

national security information, restricted data, and/or sensitive but unclassified information.